

Quantum interpolation of polynomials

Daniel M. Kane*

Samuel A. Kutin†

August 2009

Abstract

We consider quantum interpolation of polynomials. We imagine a quantum computer with black-box access to input/output pairs $(x_i, f(x_i))$, where f is a degree- d polynomial, and we wish to compute $f(0)$. We give asymptotically tight quantum lower bounds for this problem, even in the case where 0 is among the possible values of x_i .

1 Introduction

Can a quantum computer efficiently interpolate polynomials? Can it distinguish low-degree from high-degree polynomials? We consider black-box algorithms that seek to learn information about a polynomial f from input/output pairs $(x_i, f(x_i))$. We define a more general class of (d, S) -independent function properties, where, outside of a set S of exceptions, knowing d input values does not help one predict the answer. There are essentially two strategies to computing such a function: query $d + 1$ random input values, or search for one of the $|S|$ exceptions. We show that, up to constant factors, we cannot beat these two approaches.

Let \mathcal{F} be a collection of functions from some domain D to some range R . A *property* is a (nontrivial) map $\mathcal{P}: \mathcal{F} \rightarrow \{0, 1\}$. We say that \mathcal{P} is (d, S) -independent for some subset $S \subseteq D$ if, for any $z_1, \dots, z_d \in D$ with $z_1, \dots, z_r \in S$ and $z_{r+1}, \dots, z_d \notin S$ (where $r = |\{z_i\} \cap S|$), the $(d - r)$ -tuple of values $(f(z_{r+1}), \dots, f(z_d))$ is independent of the $(r + 1)$ -tuple $(f(z_1), \dots, f(z_r), \mathcal{P}(f))$. We say that \mathcal{P} is d -independent if it is (d, \emptyset) -independent. (For simplicity, we consider independence with respect to the uniform distribution on \mathcal{F} .)

For example, let \mathcal{F} be the set of degree- d polynomials from some finite field K to itself. Let $R = K$, and let D be some subset of K . We could define $\mathcal{P}(f)$ to be one bit of information about a particular function value $f(z)$. If $z \notin D$, then this property is d -independent; knowing any d values of a degree- d polynomial yields no information about any other value. If $z \in D$, then \mathcal{P} is $(d, \{z\})$ -independent. Alternatively, we could define $\mathcal{P}(f)$ to be one bit of information about a (nonconstant) coefficient of f ; this is also d -independent.

*Dept. of Mathematics, Harvard University, One Oxford Street, Cambridge MA 02138. Email: dankane@math.harvard.edu

†IDA/CCR-P, 805 Bunn Drive, Princeton NJ 08540. Email: kutin@idacccr.org

We analyze quantum algorithms that compute such a \mathcal{P} based on black-box access to the function f . We consider two models:

- In the *chosen-input* model, we give our oracle $x \in D$ and it returns $f(x)$. (More precisely, the oracle transformation maps $|x, b, c\rangle$ to $|x, b + f(x), c\rangle$, where $+$ is some appropriate reversible notion of addition.)
- In the *random-input* model, there is some map X from $\{1, \dots, n\}$ onto D . We give our oracle i and it returns the pair $(X(i), Y(i))$, where $Y(i) = f(X(i))$. This oracle is our only access to the map X .

The random-input model may seem unusual. It is a natural extension of Valiant's PAC learning model [Val84] to the quantum setting, although it differs slightly from the quantum PAC model introduced by Bshouty and Jackson [BJ99]. For technical reasons, we consider distributions on maps X with the same image D . We say that such a distribution is *permutation-independent* if, for any permutation σ on D , the maps X and $\sigma \circ X$ have the same probability.

We prove a result for each model. We say that the *bias* of an algorithm is its edge over random guessing; that is, on any input f , the algorithm outputs $\mathcal{P}(f)$ with probability at least $\frac{1}{2} + \epsilon$.

Theorem 1. *Let \mathcal{P} be a d -independent property of a family of functions \mathcal{F} . Let A be a quantum query algorithm, in the chosen-input model, which, for any $f \in \mathcal{F}$, correctly computes $\mathcal{P}(f)$ with positive bias. Then the number of queries made by A is at least $(d+1)/2$.*

Theorem 2. *Let \mathcal{P} be a (d, S) -independent property of a family of functions \mathcal{F} with a domain of size n . Let Δ be a permutation-independent distribution of random maps. Let A be a quantum query algorithm, in the random-input model, which, for any $f \in \mathcal{F}$, and with $X \sim \Delta$, computes $\mathcal{P}(f)$ with bias at least ϵ . Then the number of queries made by A is at least*

$$\min \left\{ \frac{d+1}{2}, C_\epsilon \sqrt{\frac{n}{|S|}} \right\},$$

where C_ϵ is a constant depending on ϵ .

To return to our first example, suppose \mathcal{F} is the set of degree- d polynomials, and $\mathcal{P}(f)$ is one bit of information about $f(z)$ for some $z \notin D$. One strategy is to make $d+1$ queries to compute $d+1$ different values of $f(X(i))$, interpolate the polynomial, and read off $f(z)$. The above theorems show that, for either query model, this approach is within a factor of 2 of being optimal.

What if, instead, $z \in D$? In the chosen-input model, computing $f(z)$ is no longer interesting; we can perform a single query. In the random-input model, we could still query $d+1$ points and interpolate, or we could use Grover search [Gro96] to find the value of i with $X(i) = z$, at which point one additional query gives the answer. Theorem 2 says that one of these two strategies must be optimal, up to a constant factor.

We survey lower bound methods in Section 2, focusing on the approach we will use: the polynomial method [BBC⁺]. We then prove the two above theorems in Section 3 and give some final thoughts in Section 4.

2 Lower Bound Methods

There are several standard techniques for proving quantum query lower bounds. One approach is to use information theory. For example, suppose our goal were not to compute $f(z)$ at a single point, but to produce a complete description of the degree- d polynomial f . This requires specifying $d + 1$ coefficients, each an element of K . But each query gives us, information-theoretically, at most two elements of K . By an interactive version of Holevo’s Theorem [CvDNT99, Theorem 2], we require at least $(d + 1)/4$ queries. However, this approach does not apply to computing a single value $f(z)$.

A second approach is to use the “adversary” method of Ambainis [Amb02]. The basic idea, in our setting, would be to find a collection of functions $g \in \mathcal{F}$ with $\mathcal{P}(g) = 0$, and another collection of $h \in \mathcal{F}$ with $\mathcal{P}(h) = 1$, where each g is “close to” many h , in the sense that they agree on almost all inputs. However, any two distinct polynomials disagree on almost all inputs. Høyer, Lee, and Špalek [HLS07], after noting that Ambainis’s original method cannot prove a non-constant lower bound when 0-inputs and 1-inputs disagree on a constant fraction of the inputs, propose a variant with “negative weights” that, in theory, does not run up against this barrier. In practice, even this generalized adversary method has not yet yielded a nonconstant lower bound for such a problem.

We will apply the polynomial method [BBC⁺]. For the chosen-input model, let $\delta_{x,y}$ be the function of f that is 1 when $f(x) = y$ and 0 otherwise. Then the quantum query maps

$$|x, b, c\rangle \mapsto \sum_y \delta_{x,y} |x, b + y, c\rangle.$$

So, if we start in some fixed state, after a single query each amplitude is an affine expression in the values $\delta_{x,y}$. After T queries, each amplitude is a polynomial in $\{\delta_{x,y}\}$ of degree at most T . We now measure the state and output some bit; the probability that this bit is 1 is thus a polynomial of degree at most $2T$. This polynomial p satisfies the following properties:

- If $\delta_{x,y}$ encodes any function from D to R (that is, each $\delta_{x,y} \in \{0, 1\}$ and $\sum_{y \in R} \delta_{x,y} = 1$ for all x), then $0 \leq p(\{\delta_{x,y}\}) \leq 1$.
- If $\delta_{x,y}$ encodes some $f \in \mathcal{F}$, then $|p(\{\delta_{x,y}\}) - \mathcal{P}(f)| < \frac{1}{2}$.

A lower bound on the degree of such a polynomial thus gives a lower bound on the number of quantum queries.

For the random-input model, the same idea applies; the variable $\delta_{i,x,y}$ is 1 when $X(i) = x$ and $f(x) = y$ and 0 otherwise, and

$$|i, a, b, c\rangle \mapsto \sum_{x,y} \delta_{i,x,y} |i, a + x, b + y, c\rangle.$$

The polynomial p in this setting satisfies the properties:

- If $\delta_{i,x,y}$ encodes any functions X from indices to D and Y from indices to R (that is, each $\delta_{i,x,y} \in \{0, 1\}$ and $\sum_{x,y} \delta_{i,x,y} = 1$ for all i), then $0 \leq p(\{\delta_{i,x,y}\}) \leq 1$.
- If $\delta_{i,x,y}$ encodes X and $f \circ X$ for some $f \in \mathcal{F}$, then $|p(\{\delta_{i,x,y}\}) - \mathcal{P}(f)| \leq \frac{1}{2} - \epsilon$.

In early uses of the polynomial method [BBC⁺], one step in a typical application was to symmetrize down to a polynomial in one variable. This works well for total functions, but not for promise problems. (Here, the promise is that f represent some function.) The method has been adapted to a similar setting for proving a lower bound for the element distinctness problem [AS04, Kut05]; in this case, symmetrizing separately on the domain and range yields a function of two variables. We will use a similar approach to tackle interpolation.

Remark. There are different ways to prove lower bounds on the degree of a polynomial computing a function. For example, a referee for an early version of this paper noted that Theorem 1 above can be proved using a general result¹ of Buhrman, et al. [BVdW07]. We give a direct proof whose main idea generalizes to the random-input problem.

3 Proofs

We now prove our main results. We begin with the chosen-input model.

Proof of Theorem 1. Let A be an algorithm computing the d -independent property \mathcal{P} with nonzero bias. Suppose that A makes fewer than $(d+1)/2$ queries. As discussed in Section 2, we write the probability that A outputs 1 as a polynomial $p(f)$, by which we mean a polynomial in the variables $\{\delta_{x,y}\}$, of degree at most d . When $f \in \mathcal{P}^{-1}(0)$, then $0 \leq p(f) < \frac{1}{2}$; when $f \in \mathcal{P}^{-1}(1)$, then $\frac{1}{2} < p(f) \leq 1$.

Write p as a sum of monomials $\sum_k m_k$. Each monomial has the form

$$m_k = \prod_{j=1}^t \delta_{x_j, y_j}$$

for some $t \leq d$. Hence, each m_k depends on at most d values of f . By the definition of d -independence, the expected value of m_k over $\mathcal{P}^{-1}(0)$ is the same as it is over $\mathcal{P}^{-1}(1)$. This is true for all k , so

$$\frac{1}{2} < \mathbf{E}_{f \in \mathcal{P}^{-1}(1)}[p(f)] = \mathbf{E}_{f \in \mathcal{P}^{-1}(0)}[p(f)] < \frac{1}{2}.$$

This is impossible. We conclude that no such algorithm exists; that is, any algorithm computing \mathcal{P} requires at least $(d+1)/2$ queries. \square

¹See the discussion following their Lemma 3 [BVdW07].

The proof of Theorem 2 is more involved. We will first show that, assuming an algorithm makes fewer than $(d+1)/2$ queries, the actual values of $f(x)$ do not matter unless x is in the special set S . This first part of the argument uses the same logic as the proof of Theorem 1.

Intuitively, if the values $f(x)$ matter only for $x \in S$, the simplest possible case would be one where any such value of $f(x)$ immediately yields the answer $\mathcal{P}(f)$. This is Grover search, with a known lower bound of $\Omega(\sqrt{n/|S|})$. The second part of the proof of Theorem 2 represents one approach to formalizing this intuition.

Proof of Theorem 2. Let A be an algorithm computing the (d, S) -independent property \mathcal{P} with bias at least ϵ . Suppose that A makes fewer than $(d+1)/2$ queries. As discussed in Section 2, we write the probability that A outputs 1 as a polynomial $p(X, Y)$, by which we mean a polynomial in the variables $\{\delta_{i,x,y}\}$, of degree at most d . For any i and any $x \notin S$, we introduce the variables $\xi_{i,x}$ (which is 1 when $X(i) = x$ and 0 otherwise) and $v_{i,y}$ (which is 1 when $Y(i) = y$ and 0 otherwise), and we write $\delta_{i,x,y} = \xi_{i,x}v_{i,y}$. For all $X: \{1, \dots, n\} \rightarrow D$ and $Y: \{1, \dots, n\} \rightarrow R$, we have $0 \leq p(X, Y) \leq 1$; we will use this generality. When $f \in \mathcal{F}$, we have $|p(X, f \circ X) - \mathcal{P}(f)| \leq \frac{1}{2} - \epsilon$.

Write p as a sum of monomials $\sum_k m_k$. Each monomial has the form

$$m_k = \prod_{j=1}^r \delta_{i_j, x_j, y_j} \prod_{j=r+1}^t \xi_{i_j, x_j} v_{i_j, y_j}$$

for some $r \leq t \leq d$ with $x_j \in S$ for $j \leq r$ and $x_j \notin S$ for $j > r$, and with all i_j distinct. By the definition of d -independence, once we condition on $X(i_j) = x_j$ for $1 \leq j \leq t$, the expected value of $\prod_{j=r+1}^t v_{i_j, y_j}$ over $f \in \mathcal{F}$ and $X \sim \Delta$ is independent of $\mathcal{P}(f)$ and of the values δ_{i_j, x_j, y_j} for $j \leq r$. Hence, we can replace this product with its expected value over f and X , yielding a new polynomial q using only the variables $\delta_{i,x,y}$ (for $x \in S$) and $\xi_{i,x}$ (for $x \notin S$). The polynomial q satisfies the original conditions: $0 \leq q(X, Y) \leq 1$ for any X, Y , and $|q(X, f \circ X) - \mathcal{P}(f)| \leq \frac{1}{2} - \epsilon$ when $f \in \mathcal{F}$. Furthermore, $\deg q \leq \deg p$.

If $S = \emptyset$, then q depends only on X but not f , which is impossible. In this case, A must have made at least $(d+1)/2$ queries. For the remainder of the proof we assume S is nonempty.

We now apply q to a particular set of instances. Let $k = |S|$, write $S = \{z_1, \dots, z_k\}$, and write $D \setminus S = \{z_{k+1}, \dots, z_n\}$. We will permute these values in blocks. Let $B = \lfloor n/k \rfloor$. For any function π from $\{0, \dots, B-1\}$ to $\{0, \dots, B-1\}$ we get an arrangement given by $X(i + kj) = z_{i+k\pi(j)}$ for $1 \leq i \leq k$ and $0 \leq j < B$. (We write $X(i) = z_i$ for $i > Bk$.) When π is a permutation, the list $\{X(i)\}$ covers all of D .

Now, choose some $g, h \in \mathcal{F}$ with $\mathcal{P}(g) = 0$ and $\mathcal{P}(h) = 1$. We let $Y(i + kj)$ (where $1 \leq i \leq k$) be $g(z_i)$ when j is even and $h(z_i)$ when j is odd. Fixing these values, any function π gives us values of $\delta_{i,x,y}$ (for $x \in S$) and $\xi_{i,x}$ (for $x \notin S$). We let $q(\pi)$ denote the result of applying the polynomial q to these values. It is clear that we can rewrite each $\xi_{i,x}$ or $\delta_{i,x,y}$ as 0 or as some $\eta_{i,j}$, which is defined to be 1 if $\pi(i) = j$ and 0 otherwise. Hence, $q(\pi)$ is a polynomial in $\{\eta_{i,j}\}$.

For any function π , we must have $0 \leq q(\pi) \leq 1$. For a permutation π with $\pi^{-1}(0)$ even, we have $q(\pi) = q(X, g \circ X) \leq \frac{1}{2} - \epsilon$. For a permutation π with $\pi^{-1}(0)$ odd, we have $q(\pi) = q(X, h \circ X) \geq \frac{1}{2} + \epsilon$. We have reduced to the standard problem of permutation inversion; as first shown by Ambainis [Amb02], we know that any such polynomial has degree $\Omega(\sqrt{B})$.

For concreteness, we finish the proof using symmetrization. First, we symmetrize q with respect to any rearrangement of the values $1, \dots, B-1$ in the range of π . This reduces us to variables $\{\eta_i\}$ where $\eta_i = 1$ when $\pi(i) = 0$ and 0 otherwise. Next, we symmetrize with respect to any rearrangement of even i and any rearrangement of odd i . We are left with a polynomial $q(\alpha, \beta)$ in two variables: α counts the number of even i with $\pi(i) = 0$, and β counts the number of odd i with $\pi(i) = 0$.

Note that $0 \leq q(\alpha, \beta) \leq 1$ for any $0 \leq \alpha \leq \lceil B/2 \rceil$ and any $0 \leq \beta \leq \lfloor B/2 \rfloor$. Furthermore, $q(1, 0) \leq \frac{1}{2} - \epsilon$ and $q(0, 1) \geq \frac{1}{2} + \epsilon$. We break into two cases depending on whether $q(0, 0)$ is at least $\frac{1}{2}$ or at most $\frac{1}{2}$. In either case, we get a polynomial \hat{q} in one variable with $0 \leq \hat{q}(i) \leq 1$ for $i = 0, \dots, \lfloor B/2 \rfloor$ and with a constant gap between $\hat{q}(0)$ and $\hat{q}(1)$. By a lemma of Paturi [Pat92] (see also [BBC⁺, NS94]), we conclude that $\deg \hat{q} = \Omega(\sqrt{B})$ as desired. By construction, $\deg \hat{q} \leq \deg q \leq \deg p$. \square

4 Conclusions

We have proven a lower bound of $(d+1)/2$ for polynomial interpolation (to find $f(z)$ when z is not in the domain of queries). The usual classical algorithm, of course, requires $d+1$ queries. We suspect that a quantum algorithm should also require $d+1$ queries, but we do not have a proof.

It is worth noting that, in the generality in which it is stated, Theorem 1 is tight. Let \mathcal{F} be the set of all functions from some domain to $\{0, 1\}$, and let $\mathcal{P}(f)$ be the parity $\bigoplus_{x \in U} f(x)$ of some collection of input places with $|U| = d+1$. This is a d -independent property; any set of d values, even if they all lie in U , are independent of the final answer. In this case, the standard Deutsch–Josza algorithm [DJ92] computes the parity with $(d+1)/2$ queries. Theorem 1 can be viewed as an extension of the parity lower bound of Farhi, et al. [FGGS98]. Hence, any stronger lower bound for polynomial interpolation would require using some additional structure of the problem.

The authors’ original proof of Theorem 1 did not use the polynomial method. Instead, following the same general lines as Ambainis’s proof of the adversary lower bound [Amb02], we kept track of density matrices. If, after some number of queries, we cannot distinguish 0-inputs from 1-inputs even given m additional classical queries, then after one more quantum query we cannot distinguish 0-inputs from 1-inputs given $m-2$ additional queries. The initial value of m is d , so if we make fewer than $(d+1)/2$ queries the final value is at least 0, meaning that we cannot gain any information about the answer.

The authors moved away from this proof, both because it was harder to formalize and because it did not adapt as well to Theorem 2. However, it may be that combining this original idea with the adversary method could lead to even stronger bounds on similar

problems.

Acknowledgments

The authors thank Bruce Jordan for proposing this problem. We also thank Bob Beals and David Moulton for helpful discussions.

References

- [Amb02] Andris Ambainis. Quantum lower bounds by quantum arguments. *J. Comp. Sys. Sci.*, 64:750–767, 2002.
- [AS04] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004.
- [BBC⁺] Robert Beals, Howard Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. quant-ph/9802049. IEEE Symposium on Foundations of Computer Science '98.
- [BJ99] Nader H. Bshouty and Jeffrey C. Jackson. Learning DNF over the uniform distribution using a quantum example oracle. *SIAM J. Comput.*, 28(3):1136–1153, 1999.
- [BVdW07] Harry Buhrman, Nikolay Vereshchagin, and Ronald de Wolf. On computation and communication with small bias. In *Proceedings of the 22nd annual IEEE Conference on Computational Complexity (CCC)*, 2007.
- [CvDNT99] Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Quantum Computing and Quantum Communications, First NASA International Conference, QCC '98*, number 1509 in Lecture Notes in Computer Science, pages 61–74. Springer, 1999.
- [DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London*, A439:553–558, 1992.
- [FGGS98] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Limit on the speed of quantum computation in determining parity. *Phys. Rev. Lett.*, 81(24):5442–5444, Dec 1998.
- [Gro96] Lov Grover. A fast quantum mechanical algorithm for database search. ACM Symposium on Theory of Computing (updated version), 1996. quant-ph/9605043.

- [HLŠ07] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Symposium on Theory of Computing*, STOC '07, 39th Annual ACM Symposium on Theory of Computing, pages 526–535, June 2007.
- [Kut05] Samuel Kutin. Quantum lower bound for the collision problem with small range. *Theory of Computing*, 1:29–36, 2005.
- [NS94] Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, 1994.
- [Pat92] Ramamohan Paturi. On the degree of polynomials that approximate symmetric boolean functions. In *Symposium on Theory of Computing*, STOC '92, 24th Annual ACM Symposium on Theory of Computing, pages 468–474, 1992.
- [Val84] L. G. Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134–1142, 1984.